ANTI-FRAUD POLICY
SNAITECH GROUP

April 2025

SNAITECH

INDEX

1. SNAITECH S.p.A. AND THE COMPANIES OF THE SNAITECH GROUP

SNAITECH S.p.A. is one of the main concessionaires for the management of authorised games in Italy: it offers, through its physical and online network, bets on sporting and non-sporting events, horse racing bets, betting on virtual events, video lotteries, new slots and exclusively online casino games, online slots, skill games and bingo.

SNAITECH S.p.A., at the same time, acts as the head of a Group of subsidiaries operating in the same sector of legal gaming, albeit with different functions and through different activities from those of the parent company, integrating and completing the services offered through the coordination of a retail network active throughout the country, the management of proprietary platforms (including satellite television channels) and the racetracks of Milan and Montecatini Terme.

Also part of the Group is the Snaitech Foundation - Ente Filantropico ETS - which, as an autonomous non-profit organisation, exclusively pursues social solidarity purposes in the fields of health, social assistance and charity, education and training, promotion of culture, art and scientific research, and which pertain to the protection of civil rights at the service of less affluent communities.

2. PURPOSE AND SCOPE OF THE ANTI-FRAUD POLICY

The SNAITECH Group pursues the values of honesty and legality, referring not only to national legislation, but also to the legislation in force in each country in which it operates, to EU regulations, and to any applicable international principle or convention for its reference sector.

This *policy* defines the general principles and rules of conduct on preventing and combating fraud that must be observed within the SNAITECH Group.

Each company of the SNAITECH Group adopts this *policy* and complies with the principles and rules of conduct it lays down.

The objective of this *policy* is to promote within SNAITECH S.p.A., as well as within the other Companies that make up the SNAITECH Group, the integrity of the behaviour of employees and *management*, in the belief that economic subjects cannot have good conduct without respecting ethical principles. In this context, in fact, each Company of the SNAITECH Group is required to operate in full legality and in compliance with the rules and principles of behaviour defined within the already adopted Group Code of Ethics.

In order to continue the process of strengthening and continuously improving its *governance* system with a view to consolidating the model of responsible conduct of its business, the SNAITECH Group has decided to adopt this Fraud *Policy* aimed at outlining its fraud risk governance and control model.

In particular, the anti-fraud *policy* aims to define:

- roles and responsibilities;
- the fraud risk prevention and monitoring process;
- the disciplinary system;
- signalling channels;
- the investigative process.

The scope of this *policy* extends to all the companies that make up the SNAITECH Group, i.e:

- SNAITECH S.p.A.;
- each of the subsidiaries of SNAITECH S.p.A.;
- Snaitech Foundation - ETS Philanthropic Organisation.

This *policy* is addressed to all those who - in various capacities - perform their activities in the interest of SNAITECH S.p.A., of each of its subsidiaries or of the entire SNAITECH Group (members of the administrative, supervisory and control bodies, managers, employees, collaborators in any capacity, consultants, partners, suppliers, etc.).

The contents of the *policy* are intended to be supplementary to the existing regulatory instruments constituted:

- the Code of Ethics of the SNAITECH Group, which gathers and defines the set of values and principles of conduct that must guide the operations of the entire SNAITECH Group and of each of its constituent companies;

- the Organisation, Management and Control Model *pursuant to* Legislative Decree no. 231/01 adopted by each SNAITECH Group company;
- by the SNAITECH Group's Anti-Corruption *Policy;*
- the procedures, guidelines and operating manuals adopted internally by each company to govern the conduct of its business.

3. DEFINITIONS

For the purposes of this *policy*, the terms listed shall have the meaning specified below:

SNAITECH: the company SNAITECH S.p.A.;

SNAITECH Group (or **Group**)**:** the group of companies headed by SNAITECH S.p.A.;

Subsidiaries (or **Subsidiaries**): Companies under the direct or indirect control of SNAITECH S.p.A.;

Code of Ethics**:** Code of Ethics of the SNAITECH Group;

Addressees: the staff of SNAITECH S.p.A. and its subsidiaries (members of the administrative, supervisory and control bodies, managers, employees) as well as anyone who, for any reason, works in favour of the Group or one or more of its member companies (e.g. consultants, external collaborators, partners, suppliers, etc.);

Fraud or fraudulent practice: any deceptive or intentionally misleading activity carried out in order to confuse or deceive a party, to obtain a financial or other benefit, or to avoid an obligation, for one's own benefit or that of others;

ACFE Fraud Tree: a model for exemplifying possible fraud schemes, classified into three macro-categories (bribery, embezzlement and budget fraud), developed by the *Association of Certified Fraud Examiners*;

Anti-fraud legislation: national and international legislation applicable in Italy and in the countries in which the SNAITECH Group operates;

Reporting: the reporting activity through which fraud phenomena involving the activities of the SNAITECH Group, of the companies that make it up, or of one or more persons who, for any reason, perform activities in the interest of the same Group or of each of the companies belonging to the same;

Reporting party**:** any person (inside and outside the SNAITECH Group) who makes a Report;

Reported person**:** any person to whom the facts that are the subject of a report are referred or referable;

Legal and Corporate Affairs Department (or Legal Department): the Department responsible for receiving, analysing and managing reports of fraud, except for those falling within the scope of Legislative Decree No. 24/2023 (*Whistleblowing* Decree), which will be communicated to and managed by the *Whistleblowing* Committee;

***Whistleblowing* Committee**: a body in collegiate form, specifically made up of members who are experts in the field (internal and/or external to the Companies of the SNAITECH Group), with the task of managing reports falling within the scope of application of Legislative Decree no. 24/2023 (*Whistleblowing* Decree).

4. GENERAL PRINCIPLES

The set of values and ethical principles to be complied with by anyone who, for any reason, works in favour of the SNAITECH Group or the companies belonging to it are defined in the SNAITECH Group Code of Ethics.

With a view to preventing fraud, each Addressee is required: *(i)* to act with integrity in the performance of his or her work, taking care that his or her professional conduct is not influenced by possible personal gains or advantages; *(ii)* to promptly report any doubtful episodes; *(iii)* to correctly use the tools, economic means and resources entrusted to them in any capacity; *(iv)* to perform the assigned tasks with the necessary diligence, accuracy and professionalism.

5. THE CONCEPT OF

Generally speaking, the concept of fraud covers any deceptive or intentionally misleading activity carried out in order to confuse or deceive a party, to obtain a financial or other benefit, or to avoid an obligation, for one's own benefit or for the benefit of others.

As far as corporate entities are concerned, the ACFE model classifies fraud into three macro-categories, namely bribery, embezzlement and budget fraud.

This *policy* aims to regulate fraudulent conduct referable to embezzlement, while conduct referable to corruptive schemes (for which the provisions of the SNAITECH Group's anti-corruption *policy* apply) and balance sheet fraud (which are governed by the corporate procedures and protocols identified in the Organisation, Management and Control Model adopted by the Group companies pursuant to Legislative Decree no. 231/01) are excluded.

The requirements of the *policy* refer to:

- **internal fraud**, i.e. fraudulent conduct by the staff of SNAITECH S.p.A. and its subsidiaries, regardless of their level and classification;
- **external fraud**, perpetrated by persons outside the company organisation.

Fraud' shall mean any conduct engaged in by a person who, by omitting, evading or transgressing internal rules (policies, procedures, operating instructions, etc.) and/or external rules, procures for himself or others an unfair profit to the detriment of the Company.

By way of non-exhaustive example, fraudulent conduct may be found in the case of:

- embezzlement of money: theft of cash, over-invoicing of assets, failure to remit sums due to the Concessionaire, fraudulent disbursements to employees (falsification of remuneration, fictitious expense reimbursements, etc.), falsification of cheques, embezzlement of funds before their entry in the accounts (sales and receivables);
- misappropriation of inventories and assets: use of company assets for personal use, theft, etc.
- in the context of remote gaming, the creation of so-called multiple accounts (or *chip dumping*): the use of multiple accounts at the same time (or collusion between two or more online players sitting at the same virtual table against each other), possibly even through the use of different devices and IP addresses to avoid detection;
- in the context of remote gaming, abuse in the use of gaming bonuses, e.g. by creating several accounts in order to take advantage of entry/registration bonuses;
- in remote gaming, illegitimate access to online gaming accounts (*phishing*);
- use of forged or stolen identity documents when opening gaming accounts;
- use of illegal electronic devices (e.g. *jammers*) capable of altering the regular operation of gaming machines;
- fraudulent tampering with gaming machines, resulting in the alteration of flows, e.g. by means of so-called double cards or culling;
- opening of gaming accounts by employees or operators of points of sale, in violation of the regulations in force;

- Illegal collection of bets on sporting events by employees outside the regulated gaming system.

6. PREVENTING AND COMBATING FRAUD WITHIN THE GROUP

6.1 Fraud Risk Governance

The **Administrative Body** determines the so-called "*tone at the top*" as it is responsible for promoting a corporate culture marked by principles of integrity and loyalty. This body guarantees free access to information and data useful for assessing, preventing, intercepting, detecting also *ex post* the risk of occurrence/actual realisation of fraud events to the internal functions in charge of monitoring and control (i.e. the 2nd level of control: *Risk Management* and *Compliance* and the 3rd level of control: *Internal Audit*).

The Company's management and control bodies promote a policy of fraud prevention, which they carry out through the construction and monitoring of an Internal Control and Risk Management System *that provides for the application of specific safeguards to mitigate the risk of* **fraud.**

The **Legal Department** is responsible assessing reports of potential fraud risk (where such risk is linked to one of the matters/areas of report indicated in this *policy*), initiating any investigations and examining the results, activating the competent company structures/figures to define any corrective actions/disciplinary measures. If, following the investigations, the Whistleblowing Unit considers that the matter reported falls within the scope of the *Whistleblowing* Decree, *it* will proceed to inform the *Whistleblowing* Committee within 7 (seven) days from the date of receipt of the report in order to deal with it promptly. The Whistleblower will also be informed of this procedure, while fully respecting the confidentiality of his/her identity and the content of the report.

The Legal Department is also responsible for preparing *reporting* flows to the Administrative and Control Bodies.

The **Human Resources Department** contributes to fostering a culture of prevention by means of periodic information/training activities on the risk of fraud, on the control measures in place and on the disciplinary system in force, in order to develop employee awareness of the possibility of incurring offences liable to disciplinary and/or criminal consequences in the event of conduct that does not comply with the company's procedural body, as well as with laws and regulations.

Management builds and develops the operational processes, identifying potential fraud schemes/scenarios applicable, assessing the fraud risk and the internal control system to guard against the identified risk, putting in place corrective measures (where necessary), and generally ensuring the application of the defined control measures.

Employees, irrespective of level and classification, are required to operate in compliance with the company's body of procedures and laws and regulations, and to report any suspicion of fraudulent conduct.

6.2. Sanctions System

The anti-fraud *policy* is adopted by each company of the SNAITECH Group to supplement and complete the provisions of its own Organisation, Management and Control Model. For this reason, in the event of infringements of the provisions of this *policy*, each company of the Group is required to assess the adoption of sanctions against the authors thereof, in the manner provided for by the sanctioning system defined within its own Model.

Each Model, in fact, defines a system of sanctions, in compliance with the principles of gradualness and proportionality of the sanction with respect to the actual seriousness of the fact ascertained, by means of which consequences of different kinds are envisaged depending on the type of Addressee:

- The disciplinary sanctions provided for in the applicable National Collective Labour Agreements, such as verbal or written reprimands, imposition of fines, suspension of salary up to dismissal, are applicable to employees (clerks, middle managers and executives);
- if the fraudulent conduct is attributable to Directors, Statutory Auditors or members of the Supervisory Bodies, the Administrative Body must be promptly informed, so that it can take the appropriate measures (e.g. revocation of proxies, removal from office, etc.);
- With regard to third parties under contract (suppliers, consultants, procurers, etc.), the contractual clauses indicating the effects of acts of fraud, even if only attempted (e.g. application of penalties, or termination) shall apply, if any. In any case, violation of the general principles and rules of conduct constitute a breach and may lead to termination of the contract, possibly accompanied by a claim for compensation for the damage caused to the Company or the Group.

7. RISK PREVENTION AND MONITORING PROCESS

The activities described below relate to the process of preventing and monitoring fraud risk, with the emphasis on the detection and assessment of risk, on control activities to guard against it in preventive and subsequent terms, and on monitoring activities to protect the entire system.

7.1. Business Processes and Fraud Risk Assessment

Business processes are constructed with the aim of identifying and assessing *ex ante* the theoretical applicability of possible fraud schemes/scenarios attributable to the Group's operational activities and organisational peculiarities in order to direct risk prevention, control and interception measures.

The assessment of fraud risk is left to the Department/Function Managers, who must consider the probability of occurrence of the fraudulent event, its impact, the internal control measures to mitigate the risk and the corrective/supplementary actions to be put in place.

The *Internal Audit*, *Compliance* and *Risk Management* Functions support *management* in identifying/confirming business processes potentially susceptible to fraud risk with respect to the provision of prevention elements specifically supporting and guaranteeing the Internal Control and Risk Management System in place.

The activities are carried out on the basis of international *best practices* that can be traced back to the organisational and process specificities of the Group.

7.2. Control Activities

Control activities take on relevance both in a preventive key, helping to prevent fraudulent acts from being carried out, and in a subsequent key, making it possible to intercept any anomalous situations (e.g. fraud perpetrated or fraud indicators).

Preventive control measures include, but are not limited to:

- the definition of roles and responsibilities consistent with the principle of segregation of activities;
- a system of powers and authorisation levels consistent with the organisational model defined;
- a system for authorising and monitoring access to corporate assets and information systems;
- traceability of processes whose activities must be verifiable, documented and traceable over time.

Subsequent control measures include:

- *internal auditing* activities;
- *data mining* analyses to identify possible anomaly indicators on which to focus attention;
- the reporting system.

In addition to the above control measures, deterrence (or *fraud* deterrence) is the process of deterring the perpetration of fraudulent acts through:

- the definition of an explicit and disclosed *fraud risk governance;*
- the creation of an anti-fraud culture;
- carrying out periodic *risk assessment* activities;
- the implementation of anti-fraud controls;
- taking a stand against fraudulent acts identified as a result of investigative activities.

7.3. Monitoring Activities

Periodic monitoring activities are carried out by the *Internal Audit* Function, which, with respect to the evidence that emerges, requests each of the competent Departments/Functions to indicate the corrective actions and control measures implemented to address the *gaps* identified.

Appropriate reports are prepared and submitted to the attention of the SNAITECH Group's top management and administrative and control bodies.

8. SIGNALLING CHANNELS

8.1. Reporting modalities

Recipients who have evidence - or have a well-founded suspicion - of violations of this *policy* or of any action that may point to the risk of fraud may report the incident to the Legal Department.

The Legal Department will analyse the report received (also with regard to its truthfulness and groundedness) and will handle it, activating, if necessary, the competent corporate structures/figures to define any corrective actions/disciplinary measures.

If, following further investigation of the report, the Legal Department considers that the matter reported falls within the scope of the *Whistleblowing* Decree, it will proceed to inform the *Whistleblowing* Committee within and no later than 7 (seven) days from the date of receipt of the report. The *Whistleblowing* Committee - established at each company of the SNAITECH Group - shall handle the report in accordance with the procedures and prescriptions defined in the relevant *Whistleblowing policy*, also through the Information Channel for internal reports made available by each company, in compliance with the principles of confidentiality and privacy.

The Whistleblower will be promtly informed of all the above, while fully respecting the confidentiality of his or her identity and the content of the report.

Whistleblowers may forward their report to the Legal Department through the channels indicated below:

- E-mail to the address: segnalazionefrode@snaitech.it
- Ordinary mail sent to the address of the Company's registered office -Via Vittor Pisani, 22, Milan, 20124 - to the attention of the Legal Department.

At the same time, the addressees of this policy who consider that they have been subjected to retaliatory behaviour (e.g. a threat of dismissal, demotion, etc.) for refusing to take part in acts whose fraudulent matrix they have recognised, must send a similar report bringing what happened to their attention to the attention of the same Legal Department.

9. CONDUCT OF INVESTIGATIONS

The initiation of internal investigations may result from numerous events, including but not limited to:

- reports through the *whistleblowing* IT channel or alternative channels;
- information gathered as a result of *internal auditing* activities;
- suspicious anomaly indicators;
- official communications or investigative activities by the judicial authorities.

If, on the other hand, the investigation establishes violations on the part of employees, members of administrative or control bodies or third parties, the Legal Department/Whistleblowing Committee shall refer the matter to the Company's Administrative Body and the competent company structures/figures for the definition of any disciplinary and/or legal measures.

10. TRAINING DUTIES

The SNAITECH Group and the companies that are part of it, each with reference to its own sphere of operation, must recognise and assess the risk of fraud and, where necessary, provide for specific rules of conduct for the reference company through the adoption of specific internal regulatory documents (procedures, policies, operating manuals, etc.). Each company is required to provide adequate assistance so that the addressees of this policy are put in a position to comply with its provisions.

10.1 Delivering training to staff

As part of staff training programmes, training sessions on preventing and combating fraudulent conduct must be provided, to be delivered either through face-to-face training sessions or, alternatively, by using e-learning technologies.

The training programme must cover:

- the risks of fraud to which the SNAITECH Group, its member companies and each of the addressees of this policy are exposed;
- the prevention policy adopted internally within the Group;
- preventive actions to be taken and reports to be made in relation to the risk or suspicion of the occurrence of fraudulent phenomena.

The training programmes and attendance reports for these training sessions must be kept.

10.2. The prevention of fraudulent phenomena in external relations

Third parties, suppliers and consultants must be informed of the adoption of this policy and they must be required, in their relations with the SNAITECH Group and/or with each of the companies belonging to it, to scrupulously comply with its provisions.